Bij de bodem beginnen: de AVG

Mei 2018 staat voor de deur. Twee jaar na het in werking treden van de AVG is deze vanaf aankomende 25 mei 2018 ook van toepassing. De AVG vereist dat organisaties een aantoonbaar proces hebben voor de juiste omgang met persoonsgegevens. De omvang van mogelijke boetes van toezichthouders, het recht van personen om compensaties te eisen bij onrechtmatige handelingen, de aansprakelijkheid van bestuurders van organisaties en de opkomst en effectiviteit van cybercriminaliteit dwingt de verantwoordelijke bestuurder van elke organisatie onmiddellijk een risicoanalyse (organisatie PIA) te maken om te beoordelen waar vanuit het gezichtspunt van persoonsgegevensbescherming de risico's in de organisatie zitten.

Introductie

Artikel 8 van het Europees Verdrag voor de Rechten van de Mens geeft elk mens het recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Omdat elk gebruik van persoonsgegevens een inperking van dit recht van bescherming van de persoonlijke levenssfeer kan inhouden is het gewenst dat er regels zijn rondom het zorgvuldig gebruik maken van persoonsgegevens. De Organisatie voor Economische Samenwerking en Ontwikkeling (OESO/OECD) heeft in 1980 acht privacy principes gedefinieerd[1]. Deze principes vormen de basis van de europese richtlijn en verordening.

Tot mei 2016 werd het raamwerk binnen de Europese Gemeenschap bepaald door de in 1995 ondertekende Europese richtlijn[2]. De lidstaten werden verondersteld de hierin opgenomen bepalingen in hun eigen nationale Wet- en regelgeving op te nemen. In nederland heeft dit geresulteerd in de Wet Bescherming Persoonsgegevens[3] die op 1 september 2001 in werking is getreden. Omdat er verschil van interpretatie bestond is deze richtlijn door verschillende EU lidstaten op verschillende wijze opgenomen in hun nationale wetgeving, wat resulteerde in een inconsistente lappendeken van dataprotectie regels in de EU.

Om binnen de EU één markt met vrij verkeer van personen, goederen en gegevens te creëren is een nieuw EU dataprotectie raamwerk van kracht geworden in Mei 2016: de Algemene Verordening Gegevensverwerking (AVG)[4]. Omdat het hier gaat om een Europese verordening hoeven de EU lidstaten hun lokale wetgeving niet aan te passen om de regels van kracht te maken. De verordening geldt automatisch binnen alle EU landen.

Toch zijn er nog een paar gebieden waarbinnen de EU lidstaten vrij zijn om eigen (afwijkende) nationale wetgeving op te nemen (zoals in nederland zeer waarschijnlijk de opname van het BSN nummer als bijzonder persoonsgegeven) er zal er dus ongetwijfeld enige variatie in de dataprotectie regels blijven bestaan tussen de EU lidstaten. Hierbij geldt dat de AVG de minimale bescherming beschrijft, en er alleen strengere regels mogen worden bepaald binnen een lidstaat.

De AVG dwingt een aantoonbare bedrijfsbrede strategie af rond het beheersen van persoonsgegevens, van verzamelen tot vernietiging. Door de verplichte aantoonbaarheid is een aanpak gebaseerd op een afstreeplijst niet voldoende. Er is ook geen "silver bullet' waarmee elk bedrijf de verplichtingen binnen de AVG na kan komen, de hoeveelheid werk die je moet doen

1 http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#guidelines
2 http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:31995L0046&from=NL
3 http://wetten.overheid.nl/BWBR0011468/2017-07-01
4 http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=OJ:L:2016:119:TOC

varieert nogal, afhankelijk van de omvang van de organisatie en de huidige aanpak en processen. U kunt, bijvoorbeeld, een nieuwe procedure moeten inrichten om met de AVG's "privacy by design" eis om te kunnen gaan, of nieuwe voorzieningen moeten maken rond transparantie en de rechten van het individu. En het kan voorkomen dat uit een beoordeling van proportionaliteit en subsidiariteit van een verwerking blijkt dat er in het verleden te veel gegevens zijn verzameld. Overigens kan uit een beoordeling ook komen dat er meer gedaan kan en mag worden met de verzamelde gegevens. De AVG geeft duidelijke kaders aan waarbinnen gegevensverwerkingen mogelijk zijn. Hierdoor kan het, mits transparant voor betrokkenen, ook mogelijk zijn om de verzamelde gegevens vaker en breder in te zetten in bedrijfsprocessen.

De AVG vereist dat elke verwerking van persoonsgegevens rechtmatig, behoorlijk en transparant is. Dus voor een welbepaald doel, vanuit één van de zes grondslagen, subsidiair en proportioneel. Ook dat de gegevens juist en volledig worden gehouden, niet langer worden bewaard dan strikt noodzakelijk, dat de gegevens passend worden beveiligd, en dat de verantwoordelijke voor de verwerking zijn plicht neemt in de uitvoering van deze beginselen.

Het is daarom van groot belang voor directieleden, werknemers en leidinggevenden dat men begrijpt hoe de dagelijkse gang van zaken – op elk niveau - kan worden beïnvloed door de AVG. Bedrijfsmanagers zullen moeten bepalen welke persoonsgegevens momenteel worden verzameld met welk doel en op welke grondslag, waar deze worden opgeslagen, hoe deze door de organisatie stromen, met wie ze worden gedeeld, hoe ze worden beveiligd en of derden er toegang tot moeten hebben. In een grote complexe organisatie bijvoorbeeld, kan de voorbereiding op de AVG behoorlijke gevolgen hebben voor zaken als budget, informatietechnologie, personeel, de manier waarop het bedrijf wordt geleid en hoe er wordt gecommuniceerd. en kunnen extra tijd en middelen nodig zijn voor de implementatie.

De AVG legt sterker de nadruk op de documentatie die de verantwoordelijken – degenen die bepalen wanneer, hoe en met welk doel persoonsgegevens zullen worden verwerkt – moeten bijhouden om hun aansprakelijkheid aan te kunnen tonen. Het nakomen van de AVG gaat van organisaties vereisen dat ze hun huidige aanpak rond de aansturing van de organisatie herzien en de analyse maken hoe gegevensbescherming aangepakt gaat worden als een bedrijfsbelang. Afhankelijk van de organisatie en de verzamelde gegevens kan het verplicht danwel wenselijk zijn een zogenoemde Functionaris Gegevensbescherming (FG/DPO) aan te stellen. De rol, positie en kennis van deze functionaris is omschreven in de AVG en een adviesrapport[5] van de Article 29 Working Party (WP29). Deze Working Party is het samenwerkingsverband van de voor Data Protectie Autoriteiten (DPA's) van de lidstaten. Voor Nederland is de Autoriteit Persoonsgegevens hierin vertegenwoordigd.

Een aspect hiervan kan zijn dat alle contracten en andere overeenkomsten die er zijn rond het delen van informatie met andere organisaties moeten worden herzien, inclusief die rond cloud diensten en uitbesteed werk. Het is van groot belang om om zo snel mogelijk te beginnen met planning en om de medewerking te verkrijgen van de leidinggevenden binnen uw organisatie. We bieden in dit document een overzicht van de belangrijkste zaken die moeten worden aangepakt met het oogmerk inzage te kunnen geven in de taken die voor hen liggen.

5 ec.europa.eu/newsroom/document.cfm?doc_id=44100

Wat alle organisaties ten minste moeten overwegen

De straffen voor overtredingen zijn gelijk getrokken binnen de EU

Onder de huidige dataprotectierichtlijn was het zo dat EU lidstaten zelf konden bepalen hoe hoog de maximumboete was. Hierdoor ontstonden grote verschillen tussen EU lidstaten: het maximum kan in Oostenrijk oplopen tot € 25,000, maar in Frankrijk tot € 150.000, in Spanje tot € 600.000 of £ 500.000 in het Verenigd Koninkrijk. Er zijn een aantal zaken waarbij schending van de privacy grote internationale bedrijven hoge boetes hebben opgelegd. De spaanse DPA heeft recent een boete van 1.2 miljoen euro geëist in een zaak tegen Facebook. In nederland heeft de autoriteit persoonsgegevens tot nu toe het recht om als maximale boete 10% van de jaaromzet op te leggen als Last onder dwangsom.

Artikel 85(5) van de AVG stelt Autoriteit Persoonsgegevens in staat om boetes tot ten minste € 20 miljoen op te leggen, of 4% van de wereldwijde omzet die het in overtreding zijnde bedrijf in het vorige financiële jaar heeft behaald als dat meer is. Aanvullend kunnen individuen nu hun recht op bescherming van hun gegevens afdwingen: artikel 82(1) van de AVG borgt dat een persoon die materiële of immateriële schade heeft geleden ten gevolge van de verwerking van zijn persoonsgegevens compensatie mag eisen. Ook kunnen groepen van natuurlijke personen hun zaken bundelen om tot een groepsvordering te komen

De definitie van “persoonsgegevens” is gelijk getrokken

Onder de AVG is de definitie van "persoonsgegevens" breder gemaakt dan in een aantal landen eerder in lokale wetgeving hadden staan. Artikel 4(1) zegt dat een persoonsgegeven alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon is (de betrokkene); een identificeerbaar natuurlijk persoon is iemand die geïdentificeerd kan worden, direct of indirect, in het bijzonder door verwijzing naar een identificerend kenmerk zoals een naam, een identificatienummer, locatiegegevens, een on-line kenmerk of aan de hand van één of meer factoren die specifiek zijn voor de fysieke, fysiologische, genetische, mentale, economische, culturele of sociale identiteit van die natuurlijke persoon. Nieuw binnen de AVG is de expliciete benoeming van biometrische gegevens als een bijzonder persoonsgegevens. (artikel 9) Binnen de AVG is expliciet gemaakt (recital 30) dat IP adressen, (namen van) cookies, identificerende nummers van mobiele apparaten en andere soorten online identificaties gezien moeten worden als “persoonsgegevens” en dienovereenkomstig beschermd moeten worden.

De AVG heeft een groter geografisch bereik.

Artikel 3 van de AVG stelt dat de nieuwe regels gelden voor entiteiten die zijn gevestigd in de EU en de territoriale wateren die persoonsgegevens verwerken, ofwel voor eigen gebruik (als verantwoordelijke) of namens een andere entiteit (als 'verwerkers'), ongeacht of de verwerking van de data daadwerkelijk plaatsvindt in de EU. Schepen die in de territoriale wateren werken vallen hier bijvoorbeeld onder. Aanvullend stelt artikel 3(2) dat de AVG wereldwijd van toepassing is voor welke verwerking van persoonsgebonden data dan ook van personen afkomstig uit de EU als die verwerking is gerelateerd aan het aanbieden van diensten of goederen, gratis of niet, aan personen in de EU, of als het gaat om het in de gaten houden van het gedrag van EU individuen.

In de praktijk betekent dit dat elk bedrijf dat zaken doet met inwoners van de EU (zoals het vermarkten van goederen of diensten) onder de AVG regels valt, zelfs als men buiten de EU opereert en geen locatie of apparatuur heeft in de EU. Ieder die een website beheert die toegankelijk is vanaf EU gebied (iets dat gezien kan worden als het verstrekken van een gratis elektronische dienst) kan onder de AVG vallen, en zoals hierboven beschreven, zo gauw bezoekers

middels cookies, JavaScript of andere technieken worden getraceerd, is de AVG toepasbaar. Het opslaan van een IP adres in een logfile valt mogelijk ook onder de AVG, maar overweging 49[6] geeft aan dat als het opslaan van het IP adres zolang dit strikt noodzakelijk en evenredig is met het oog op netwerk- en informatiebeveiliging een gerechtvaardigd belang vertegenwoordigd.

Een register van de verwerkingsactiviteiten is verplicht

Artikel 30(1) van de AVG vereist dat verantwoordelijke en verwerkers een schriftelijke vastlegging bijhouden (dat mag in electronische vorm) van de verwerkingsactiviteiten onder hun verantwoordelijkheid, en artikel 30(4) stelt aanvullend dat een dergelijke vastlegging op verzoek aan de van toepassing zijnde Autoriteit Persoonsgegevens beschikbaar moet worden gesteld.

De vastlegging dient het volgende te omvatten:

- de naam en de contactgegevens van de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken, en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming;
- De verwerkingsdoeleinden;
- Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- De categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;
- indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en waar van toepassing de documenten inzake de passende waarborgen;
- indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
- indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen die genomen zijn om de data te beschermen.

Als aan bovenstaande voorwaarden niet wordt voldaan voorziet artikel 83(4) van de AVG in een administratieve boete met een maximum van ten minste € 10 miljoen of, mocht dat meer zijn, 2 procent van de wereldwijde omzet zoals gemaakt in het laatste financiële jaar.

De verordening stelt dat de vastlegging niet nodig is voor kleine organisaties (minder dan 250 werknemers), maar we kunnen verwachten dat veel kleine- en middelgrote organisaties toch aan de eis tot vastlegging moeten voldoen en wel wanneer:

- De verwerking waarschijnlijk in een risico voor de rechten van de werknemers resulteert (bijvoorbeeld bijhouden van tellers, uitgebreide monitoring, vergroot risico ontstaan door ongeautoriseerde vrijgave of toegang tot gegevens, gebruik van nieuwe technologieën);
- De verwerking structureel is; of
- De verwerking speciale categorieën van gegevens omvat zoals beschreven in artikel 9(1) (bijvoorbeeld gegevens over de gezondheid, biometrische data, gegevens rond politieke of filosofische overtuiging) of persoonsgebonden data in relatie tot criminele overtuigingen en misdrijven zoals benoemd in artikel 10 van de AVG.

6 https://gdpr-info.eu/recitals/no-49/

Nieuwe gebruikersrechten moeten worden geïmplementeerd

Zoals in artikelen 13-22 is verbijzonderd dienen organisaties zeker te stellen dat effectieve systemen en processen aanwezig zijn om de volgende rechten te borgen:

1. Het recht om te worden geïnformeerd
2. Het recht op toegang
3. Het recht op correctie
4. Het recht op wissen (het 'recht om te worden vergeten')
5. Het recht om verwerking te beperken
6. Het recht op het overdragen van gegevens ('portability')
7. Het recht om bezwaar te maken
8. Rechten met betrekking tot geautomatiseerde besluitvorming en profilering.

Organisaties moeten, bijvoorbeeld, beleid hebben om te kunnen bepalen wanneer bepaalde data niet langer bewaard hoeft te worden; hoe personen in staat worden gesteld toestemming in te trekken en hoe om te gaan met verzoeken van gebruikers die bezwaar maken tegen verwerking van hun gegevens. Het verwijderen van dergelijke gegevens zal, gegeven dat bedrijfsdata vaak wordt gearchiveerd in plaats van gewist en de omvang van deze bedrijfsgegevens, nog een hele uitdaging zijn. Bij een verzoek tot vergetelheid moet op alle plaatsen waar de relevante gegevens van de persoon zich bevinden deze gegevens worden gewist. Dit betekent dus ook in backups, in papieren dossiers etc.

Technische en organisatorische [beveiligings] maatregelen zijn verplicht

De AVG vereist dat verantwoordelijke (degenen die bepalen wanneer, hoe en met welk oogmerk persoonsgegevens verwerkt zullen worden) om “passende technische en organisatorische beschermingsmaatregelen” te nemen om de persoonsgegevens die zij onder hun beheer hebben te beschermen tegen risico's die bij verwerking van gegevens aanwezig zijn, in het bijzonder “de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens”.

Artikel 32 geeft voorbeelden van de beveiligingsmaatregelen die worden verwacht:

- de pseudonimisering en versleuteling van persoonsgegevens;
- Het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- Een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Gegevensbeschermingseffectbeoordelingen (PIA's) zijn (soms) verplicht

Gegevensbescherming dient bij het ontwerp van systemen standaard meegenomen te worden en privacyeffectbeoordelingen (privacy impact assessments, of PIA's) of, zoals ze in de AVG worden genoemd "Gegevensbeschermingseffectbeoordelingen" (data protection impact assessments (DPIAs)) zijn nu verplicht (artikel 35) voor technieken en processen die waarschijnlijk kunnen leiden tot een hoog risico voor de rechten van personen (bijvoorbeeld gegevensanalyse die kan leiden tot besluiten die juridische consequenties kunnen hebben voor betrokkenen, of in het geval van bulk verwerking van gegevens). De Autoriteit Persoonsgegevens kan specifieke situaties benoemen waarvoor een DPIA wel of niet verplicht is, maar de meeste organisaties dienen, als onderdeel van hun *privacy-by-design* en algemeen gangbare strategie zeker te stellen dat een gegevensbeschermingseffectbeoordeling in het vervolg onderdeel uitmaakt van hun risico-analyse proces.

Lekken van persoonsgegevens moeten worden gemeld

Het blijft verplicht (artikel 33 van de AVG) voor een organisatie om elk lek van gegevens binnen 72 uur na het bekend worden van het lek te rapporteren aan de Autoriteit Persoonsgegevens en mogelijk aan de betrokkenen. Als daaraan niet kan worden voldaan dient het uiteindelijke rapport vergezeld te gaan van een verklaring voor de vertraging. De melding dient gedaan te worden in een specifiek formaat dat een vereiste omvat om de maatregelen te beschrijven die worden genomen om het lek te dichten en de mogelijke gevolgen ervan te beperken.
Indien het lek kan leiden tot een hoog risico voor de rechten en vrijheden van personen dient men "zonder onredelijke vertraging nadat hij er kennis van heeft genomen" het lek te melden. Deze melding is niet nodig als voldoende beschermende maatregelen - zoals versleuteling – aanwezig zijn om gevaar voor de betrokken personen te voorkomen.

Een functionaris gegevensbescherming is verplicht voor sommige organisaties

In bepaalde omstandigheden kan een organisatie verplicht zijn om een functionaris gegevensbescherming te benoemen (Data Protection Officer, DPO), bijvoorbeeld wanneer de "kerntaken" van de organisatie het in de gaten houden van grote groepen personen omvat of wanneer er bulkverwerking plaatsvindt van "speciale categorieën van gegevens" (bijvoorbeeld iemands ras of etnische afkomst, politieke overtuiging, religieuze of filosofische overtuiging, lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens indien ze worden gebruikt om een natuurlijk persoon uniek te identificeren, gezondheid, sexleven of sexuele oriëntatie). Hiernaast kan het voor organisaties nuttig zijn om in de organisatie een Privacy Officer rol te benoemen.

Samenvatting

De AVG is al in werking en wordt vanaf mei 2018 gehandhaafd. Die datum nadert met rasse schreden dus is het nodig om de resterende tijd te gebruiken om zich op de nieuwe vereisten voor te bereiden. Het bereik van de vereisten is groot; de AVG dwingt een bedrijfsbrede strategie af voor - en revisie van - processen om persoonsgegevens te beheren op elk niveau, en definieert verschillende soorten online gegevens als 'persoonsgebonden'. Er moet worden voldaan aan nieuwe rechten en verplichtingen en elke organisatie dient zijn eigen benadering uit te werken waarin de context en praktijken van het bedrijf weerspiegelen. Het is cruciaal dat het beheren van het plan van aanpak om te gaan voldoen aan de AVG een top-prioriteit krijgt op de agenda's van het bestuur en de hoogste leidinggevenden.

Dit document is opgesteld door leden van de *(ISC) 2 EMEA Advisory Council GDPR Task Force*. Hoofdauteurs: Yves Le Roux, CISSP, CISM; Paul Lanois, CCSK, CIPM, CIPT, CIPP (A, E, US and C), FIP, CISMP and LLM. Gereviseerd door Dr. Adrian Davis, MBA, FBCS CITP, CISSP; Sam Berger, CISSP; Michael Christensen, CISSP, CSSLP, CISM, CRISC, CIS LI, EU-GDPR-P; CCM, CCSK, CPSA, ISTQB, PRINCE2, ITIL, COBIT5; Ramon Codina, CISSP; Santosh Krishna Putchala, CISSP. Vertaling in het Nederlands: Heinrich W. Klöpping, MSc CISSP CCSP. Aangevuld en aangepast aan de nederlandse situatie door Jacques Eding MSc RE FIP CIPP/E CIPM CIPT CISSP CISA CISM